Universidad Carlos III de Madrid

Escuela Politécnica Superior

Ingeniería Técnica de Telecomunicación:

Sonido e imagen

Proyecto Fin de Carrera

Evaluación de prestaciones de una red mallada basada en los dispositivos Linksys WRT54GL

Autor: Francisco Ramos Santos

Tutor: Pablo Serrano Yáñez-Mingot

24 de Julio de 2009

PROYECTO FIN DE CARRERA

Departamento de Ingeniería Telemática

Universidad Carlos III de Madrid

Título: Evaluación de prestaciones de una red mallada basada en los dispositivos Linksys WRT54GL

Autor: Francisco Ramos Santos

Tutor: Pablo Serrano Yáñez-Mingot

La lectura y defensa de presente proyecto fin de carrera se realizó el día 24 de Julio de 2009 bajo el tribunal:

- **Presidente:** Ignacio Soto Campos
- **Secretario:** Norberto Fernández García
- **Vocal:** Matilde P. Sánchez Fernández

Habiendo obtenido la calificación de:

Presidente **Secretario** **Vocal**

Agradecimientos

Ahora que todo parece llegar a su fin, no puedo dejar de dar las gracias a todos cuantos me han apoyado en estos años de esfuerzo y sacrificios, de golpes y de logros.

Todos empezamos (y yo no seré una excepción) por agradecer a nuestros padres. Sé que sin su ayuda nunca habría llegado hasta aquí, así que, gracias por facilitarme el camino y por entender cada día el trabajo que he realizado.

Mis hermanos no son menos, gracias también a ellos, por entenderme en época exámenes y demás, en mis momentos buenos y más aún en mis momentos malos.

Tampoco puedo olvidarme de mis compañeros, en especial de Félix y Alberto, hoy más amigos por los cursos pasados y tras realizar prácticas, trabajos, exámenes... En definitiva por apoyarnos unos a otros en los suspensos y por las celebraciones en los aprobados.

Resaltar un agradecimiento a mi tutor Pablo Serrano y a la ayuda de Carlos J. Bernardos porque sin ellos este proyecto no habría tenido ni principio ni fin, gracias a ambos por confiar en mis capacidades y haberlas pulido para poder ser capaces de dar cuerpo al proyecto que hemos acabado.

Por último dar gracias a mi novia, Ayira, porque su apoyo incondicional desde que empezamos me ha dado moral para no hundirme, para encontrar el camino cuando más perdido he estado.

Sé que he dejado muchos nombres entre profesores y amigos. También agradecerles por formar parte de mi formación y hacer que haya conseguido la meta de terminar la carrera.

Gracias a todos.

Índice general

Índice de figuras

Índice de cuadros

Resumen

En la actualidad está emergiendo una nueva tecnología en redes inalámbricas en la cual podemos interconectar varios puntos de acceso Wi-Fi (también llamados nodos) y formar una mesh o malla de conexión que proporciona una amplia cobertura.

Las redes mesh (WMNs), o redes en malla, son aquellas redes en las que se mezclan las dos topologías de las redes WiFi. Básicamente son redes con topología de infraestructura, pero que permiten unirse a la red a dispositivos que, a pesar de estar fuera del rango de cobertura de los puntos de acceso (AP) o nodos, están dentro del rango de cobertura de algún dispositivo WiFi que directamente o indirectamente está dentro del rango de cobertura del AP. También permiten que los dispositivos WiFi se comuniquen, independientemente del AP, entre sí; es decir, los dispositivos que actúan como emisores pueden no mandar directamente sus paquetes al AP sino que pueden pasárselos a otros dispositivos WiFi para que lleguen a su destino.

Este tipo de redes desempeñarán un papel importante en la nueva generación de sistemas de comunicación ya que se puede crear una red muy amplia con buena cobertura debido a lo explicado en el párrafo anterior.

Es muy importante hacer pruebas en entornos y despliegues reales ya que en estos casos se tendrá que tener en cuenta factores que afectan al rendimiento de la red. Tales factores son el ruido, las interferencias y las limitaciones de los dispositivos reales. Por todo ello, para entender los límites de esta tecnología (mesh), hacen falta despliegues experimentales.

Para este proyecto se pretende elaborar un testbed a partir de una red formada por veinticuatro routers dispuestos bajo el falso suelo de un laboratorio de la universidad. Usamos el falso suelo ya que presenta la ventaja de

no molestar a nadie con los dispositivos y ya que de ese modo se dispone de espacio para dichos dispositivos y los cables necesarios para formar la red. Dado que el coste es un factor clave de los despliegues de una red, se usan routers comerciales como son los Linksys WRT54GL. Este despliegue contará con dos PCs que serán utilizados para controlar y supervisar todos los routers, así como también serán las fuentes de tráfico de varias pruebas.

Capítulo 1

Introducción

1.1 Motivación del Proyecto

En las redes inalámbricas el medio de transmisión es radio, es decir, sin cables. Una red que no necesita cableado es muy flexible (a cambios, añadir terminales...), además el cableado puede ser caro o complicado de realizar en instalaciones construidas sin tenerlo en cuenta, la instalación de una red inalámbrica no precisa planificación y se realiza en poco tiempo, permite la movilidad de los terminales dentro de una zona delimitada y, además, es robusta ante desastres naturales (terremotos, incendios, etc).

Dentro de este marco que engloba a las redes inalámbricas hay un tipo de redes que será objeto de estudio en este proyecto. Este tipo de redes son las redes mesh. Las redes mesh, brevemente explicadas, son redes inalámbricas multisalto con infraestructura. Como redes ad hoc inalámbricas, pero con nodos que disponen de alimentación y/o conectividad cableada a una red de datos. Este tipo de redes han atraído la atención en el mundo de las redes inalámbricas cada vez más desde los últimos años.

La tecnología mesh utiliza los estándares establecidos de una forma totalmente novedosa. El conjunto de nodos proporciona una zona de cobertura inalámbrica muy extensa. Los nodos son capaces de establecer comunicación entre ellos en cuanto sus zonas de cobertura se solapan entre sí. Por otro lado, si se solapan varias zonas de cobertura, aunque fallen uno o más nodos, la red se sustenta y sigue operando.

Tal es el auge de las redes mesh que actualmente se está trabajando para crear nuevos estándares para garantizar que se entrega buena calidad sobre el enlace wifi. Un ejemplo claro de desarrollo de estos nuevos estándares, de los que se hablará con algo más de detalle en apartados posteriores, es el 802.11s que está orientado a redes mesh, extiende el estándar MAC para soporte tanto broadcast, multicast y unicast además de otras muchas mejoras.

La mayoría del trabajo es teórico, faltan despliegues reales que permitan conocer las limitaciones de este tipo de redes, con lo cual realizar un testbed real de una red mesh hecha a partir de dispositivos comerciales dará información interesante sobre las cualidades de este tipo de redes.

1.2 Objetivos del proyecto

Los objetivos de este proyecto son construir una red mesh usando los routers Linksys WRT54GL. Para el análisis se modificarán parámetros tales como canal, rate, así como también se tendrá en cuenta la variable temporal. Es decir las horas del día y los días de la semana para saber cuando son los momentos en los que nuestras pruebas se ven afectadas por tráfico de otras redes cursado en el mismo canal o canales adyacentes.

Para realizar estas pruebas existe un paso previo que es el despliegue. Para el despliegue se usarán routers comerciales a los cuales se les efectuará un flasheo para dotarles de un firmware con mayores prestaciones que el original. Una vez realizada esta tarea se lleva a cabo el despliegue en sí, en el cual los routers irán debajo del falso suelo del laboratorio. Todos los routers deben estar conectados entre sí. Esto se hará a partir de switches. Al cual tambien se conectarán dos PCs para la gestión de los routers, además de servir para realizar diversas pruebas en las que se mandará tráfico generado de un PC a otro PC haciendo el testbed lo más real posible.

1.3 Estructura del proyecto

La presente memoria del proyecto está estructura como se expone a continuación:

- **Capítulo 1: Introducción**

  Explicación de el por qué se decide hacer este proyecto y cuales son los objetivos marcados.

  - *Capítulo 1.1: Motivación del proyecto*

    Introducción general del proyecto y resumen del porque de hacer este estudio.

  - *Capítulo 1.2: Objetivos del proyecto*

    Donde se definen los objetivos que pretendemos alcanzar.

  - *Capítulo 1.3: Estructura del proyecto*

    En este apartado se ve una estructura del proyecto donde se describe brevemente cada apartado.

- **Capítulo 2: WLAN Redes Inalámbricas**

  Presentación de las tecnologías a las cuales el proyecto se refiere. En este caso redes inalámbricas LAN.

  - *Capítulo 2.1: Topologías de red*

    Resumen sobre las topologías de redes inalámbricas existentes y proliferación en los últimos años.

  - *Capítulo 2.2: 802.11*

    Se describen los estándares 802.11 de IEEE, se resumen los niveles inferiores del modelo OSI (capa física y capa de enlace) para las conexiones inalámbricas, así como una breve descripción de la familia de especificaciones desarrolladas por la IEEE que se consideran interesantes para la ubicación conceptual del proyecto.

- **Capítulo 3: Entorno de trabajo**

  Escenario para llevar a cabo el estudio realizado, resumen de los dispositivos usados y explicación de los pasos seguidos para crear una red inalámbrica local en modo adhoc.

  - *Capítulo 3.1: Tarjeta inalámbrica Atheros*

    Se explica como configuramos la tarjeta inalámbrica Atheros para poder usarla en los PCs con el fin de monitorear el tráfico wifi.

  - *Capítulo 3.2: Linksys WRT54GL*

    En este capítulo se describen las características de los dispositivos usados (routers Linksys WRT54GL), así como también se describe el firmware instalado.

  - *Capítulo 3.3: Herramientas utilizadas*

    Herramientas que hemos utilizado así como las pruebas realizadas y los resultados obtenidos.

  - *Capítulo 3.4: Despliegue*

    Resumen de red mesh con sus principales ventajas e inconvenientes y como la hemos implementado en el laboratorio.

- **Capítulo 4: Estudio de prestaciones**

  Definimos el escenario y las pruebas realizadas.

- **Capítulo 5: Conclusiones y trabajos futuros**

  En esta parte exponemos las conclusiones sacadas al haber elaborado el proyecto y enfocamos como podrían ir trabajos futuros en la misma línea de este proyecto.

Capítulo 2

WLANs y redes malladas basadas en 802.11

Las redes inalámbricas son caracterizadas por su medio de transmisión: sin cables. Este medio puede ser bien via radio o bien via infrarrojo, aunque lo más normal es que el medio sea radio. Las redes locales se caracterizan por tener una distancia de cobertura pequeña, alrededor de 50 m dentro de un edificio.

Gracias a la primera característica de este tipo de redes llega el auge empujado por el abaratamiento de la tecnología y el mayor uso de los dispositivos que usan esta característica. Existen otras características como la flexibilidad y la no necesidad de planificación, pudiendo crear redes de ordenadores de una forma rápida, muy útiles para equipos móviles o para instalaciones temporales. Además el cableado puede llegar a ser caro o complicado de realizar en instalaciones construidas sin tenerlo en cuenta. Y, por si fuera poco, es robusto ante desastres naturales como los terremotos o los incendios.

Aunque las redes inalámbricas tienen ciertas desventajas sobre las tradicionales: poseen un ancho de banda menor, las WLANs usan espectro siendo éste un recurso limitado y sufren interferencias con aparatos eléctricos.

Las redes inalámbricas definen dos topologías de red: red independiente o adhoc y red con infraestructura. Se hablará de redes mesh, para contraponerlas con las tradicionales redes adhoc y redes con infraestructura.

2.1 WLANs

En esta sección se verán las distintas topologías de red.

2.1.1 Red ad-hoc

El modo ad-hoc se utiliza para conectar clientes inalámbricos directamente entre sí, sin necesidad de un punto de acceso inalámbrico o una conexión a una red con cables existente. Una red ad-hoc consta de clientes inalámbricos que se envían los datos directamente entre sí. Ad-hoc es el modo más sencillo para formar una red. Este modo es recomendable para redes creadas de forma espontánea, sin una infraestructura específica y funcionando en un espacio y tiempo limitados.

En esta topología cada nodo forma parte de una red Peer to Peer, sólo debemos usar el mismo SSID para todos los nodos. El SSID (identificador del conjunto de servicio extendido) es un identificador de 32 caracteres en formato ASCII que muestra el nombre de la red. Es decir en el modo ad-hoc los equipos cliente inalámbricos se conectan entre sí para formar una red punto a punto en la que cada equipo actúa como cliente y como punto de acceso simultáneamente.

2.1.2 Red con infraestructura

El modo de infraestructura se utiliza para conectar equipos con adaptadores de red inalámbricos, también denominados clientes inalámbricos, a una red con cables existente. Por ejemplo, una oficina doméstica o de pequeña empresa puede tener una red Ethernet existente. Con el modo de infraestructura, los equipos portátiles u otros equipos de escritorio que no dispongan de una conexión con cables Ethernet pueden conectarse de forma eficaz a la red existente. Se utiliza un nodo de red, denominado punto de acceso inalámbrico (PA), como puente entre las redes con cables e inalámbricas. En el modo de infraestructura, los datos enviados entre un cliente inalámbrico y otros clientes inalámbricos y los nodos del segmento de la red con cables se envían primero al punto de acceso inalámbrico, que reenvía los datos al destino adecuado.

En la siguiente figura se muestra una red inalámbrica en modo de infraestructura:

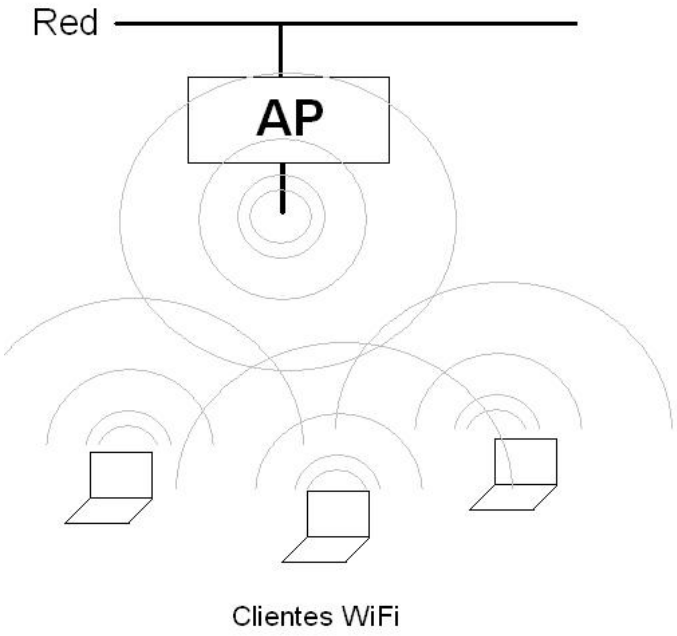

Figura 2.1: Ejemplo de un red con infraestructura

2.2 Redes MESH

Las Redes Inalámbricas Mesh (WMNs) se componen de dos tipos de nodos, los enrutadores y los clientes. Los enrutadores tienen movilidad mínima y forman el "backbone". Estas redes pueden integrarse a otras redes como Internet, IEEE 802.11, IEEE 802.15, IEEE 802.16, etc. Al contrario que los routers que forman el "backbone" los clientes pueden ser estáticos o móviles y pueden crear una red mallada entre ellos mismos y/o con los enrutadores. De este modo se mejora el rendimiento de las redes ad-hoc debido a que los nodos hacen de emisor y receptor simultáneamente consiguiendo una red con mayor robustez y dinamismo.

Una red mesh, por tanto, es básicamente una red con topología de infraestructura en la cual se pueden unir dispositivos que, aún estando fuera de la zona de cobertura del AP, están dentro de la zona de cobertura de algún

dispositivo que si está dentro de la zona de cobertura del AP, ya sea directamente o, a su vez, a partir de algún otro dispositivo. En conclusión es una red con topología de infraestructura puesto que cuenta con AP, pero usa la característica principal de las redes ad-hoc ya que los dispositivos emisores no tienen porque mandar sus paquetes directamente al AP, sino a través de dispositivos intermedios.

Normalmente los nodos disponen de múltiples interfaces para así obtener una mayor flexibilidad. Las redes mesh son vistas como una opción atractiva y de futuro, motivando trabajos como este proyecto debido a sus ventajas.

Ventajas de las redes MESH

- *Más económico:* ya que cada nodo funciona tanto como cliente como repetidor con lo cual se reduce la necesidad de torres centrales y otras infraestructuras.
- *Simplicidad:* ya que las rutas son configuradas dinámicamente.
- *Robustez:* al estar conectados a varios nodos la cada de uno de ellos no implica la pérdida de servicio para los demás.
- *La topografía:* existen terrenos rurales o urbanos en donde es difícil que todos los usuarios vean algún punto de acceso y es mucho más fácil que el usuario vea usuarios vecinos.

Limitaciones de las redes MESH

Como en cualquier tecnología las redes mesh presenta ciertas limitaciones para garantizar calidad de servicio:

- *Latencia:* retraso de los paquetes a lo largo de su camino. El número de saltos que un paquete debe dar en su camino hasta destino influye negativamente en este aspecto.
- *Rendimiento:* el ancho de banda que es capaz de ofrecer la red tambien se ve influenciado por el número de saltos que el paquete debe dar hasta llegar a destino.

- *Escalabilidad:* ya que las redes mesh no han sido aún probadas más que con algunos cientos de nodos. Se están llevando acabo estudios para que el día de mañana se lleven a cabo redes mesh que cubran ciudades o incluso países.

- *Seguridad:* en este tipo de redes así como en las redes ad-hoc se necesita reconocer y hablar con los clientes antes de conocerlos, esto constituye un reto en la seguridad de Internet.

2.3 802.11

Aunque existen varias tecnologías para crear redes inalámbricas, en este proyecto se describe el uso de los estándares 802.11 del IEEE (Instituto de ingenieros eléctricos y electrónicos). Este estándar nace para facilitar la conectividad de estaciones fijas, portátiles o móviles dentro de un área local. La norma posee muchos apartados que describen y especifican las distintas funciones que se implementan en una comunicación de datos de red. Nosotros nos concentraremos en este documento a discutir el apartado 802.11 que describe y especifica una interfaz inalámbrica para comunicaciones de datos compatibles con la Norma IEEE 802.

Dentro del apartado 802.11 se establece una subdivisión en las interfaces inalámbricas. A saber: - 802.11 a: describe una interfaz inalámbrica en la banda de 5.8 Ghz con velocidades de comunicación de datos 54 Mbps. - 802.11 b: describe una interfaz inalámbrica en la banda de 2.4 Ghz con velocidades de comunicación de datos de 11 Mbps.

La norma 802.11 b es la que actualmente se comercializa en forma masiva a través de una gran variedad de productos y aplicaciones.

El estándar IEEE 802.11 está en constante desarrollo. Existen varios grupos de trabajo encargados de proponer y definir nuevas mejoras y apéndices al estándar WLAN.

El estándar 802.11 establece los niveles inferiores del modelo OSI para las conexiones inalámbricas:

- La capa física (a veces abreviada capa ”PHY”) ofrece tres tipos de codificación de información.
- La capa de enlace de datos compuesta por dos subcapas: control de enlace lógico (LLC) y control de acceso al medio (MAC).

La capa física define la modulación de las ondas de radio y las características de señalización para la transmisión de datos mientras que la capa de enlace de datos define la interfaz entre el bus del equipo y la capa física, en particular un método de acceso parecido al utilizado en el estándar Ethernet, y las reglas para la comunicación entre las estaciones de la red.

A continuación se muestra una tabla de la familia de especificaciones que se consideran más interesantes desarrolladas por la IEEE para tecnologías de redes LAN; posteriormente explicaremos brevemente cada una de ellas:

IEEE 802.11	
Grupo de trabajo	**Enfoque**
802.11a	54 Mbps WLAN en la banda 5GHz
802.11b	11 Mbps WLAN en la banda 2.4 GHz
802.11g	54 Mbps WLAN en la banda 2.4 GHz
802.11n	Nueva generación de redes WLAN de al menos 100 Mbps
802.11e	QoS y extensiones que fluyen a través de 802.11a/g/h
802.11k	Intercambio de información de capacidad entre clientes y AP
802.11s	Define una arquitectura y un protocolo para redes Mesh
802.11v	Mejora la cantidad de energía requerida en los equipos.

Cuadro 2.1: Estándares y extensiones de 802.11

Vamos a hablar más detenídamente sobre la capa física y la subcapa MAC:

2.3.1 MAC

Control de Acceso. La capa MAC consta de dos subcapas: PCF y DCF.

1. *DCF (Distributed Coordination Function)*. Utiliza un algoritmo de contención CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance).

Si una estación desea transmitir: Escucha el medio. Si el medio está libre puede transmitir. Si el medio no está libre debe esperar a que la transmisión en curso termine. Una combinación de mecanismos de escucha físico y virtual permite determinar si el medio está libre u ocupado.

No incluye una función para detección de colisiones. El rango dinámico de las señales en el medio es muy grande y una estación no puede distinguir señales débiles del ruido, y los efectos causados por su propia transmisión.

Mecanismo: Para la adecuada operación del algoritmo se utiliza un conjunto de retardos (IFS) que configuran un esquema de prioridades:

(a) Una estación que desea transmitir escucha el medio. Si el medio está libre, espera un periodo igual IFS para ver si el medio sigue libre. Si es así, la estación transmite inmediatamente.

(b) Si el medio está ocupado (ya sea porque inicialmente la estación encontró al medio ocupado o porque el medio es ocupado durante el periodo IFS), la estación difiere la transmisión y continua monitoreando el medio hasta que la transmisión en marcha concluya.

(c) Cuando la transmisión concluye, la estación espera otro IFS. Si el medio continua libre, la estación espera un tiempo extra (backoff time) determinado de forma aleatoria. Al final de este tiempo, escucha el medio nuevamente; si el medio está aún libre, la estación puede transmitir. Si durante el tiempo extra (backoff), el medio es ocupado, el marcador del tiempo extra (backoff) es detenido, y continuará su cuenta cuando el medio sea liberado.

(d) Si la transmisión fracasa, determinado por la ausencia de un ACK, se asume que ha ocurrido una colisión.

En el caso de no tener un sistema de prioridades se tienen las siguientes imágenes:

Figura 2.2: Transmisión DCF

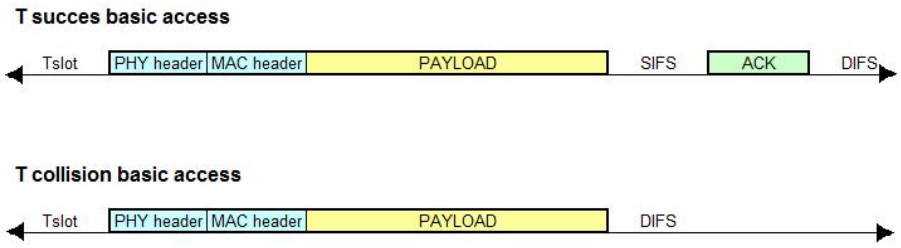

Figura 2.3: DCF acceso básico

Donde Slot o Ranura de Tiempo corresponde a un intervalo que usa la familia de protocolos IEEE 802.11 para organizar la contienda por el uso del canal. Es un valor definido entre (0, CWmin) y se obtiene como

(CWmin-1)/2 * Tempty = Tslot

A continuación se muestra una tabla con los parámetros de IEEE 802.11b y 802.11g[1]:

2. *PCF (Point Coordination Function) /basado en prioridad*. No ha sido implementado por los fabricantes. Provee transferencia de tramas sin contención. No se compite por el medio, el coordinador "coordina el acceso". Se pueden tener las dos opciones en operación simultáneamente: DCF y PCF.

[1]Los parámetros para 802.11g pueden ser distintos si lo que se busca es la mayor compatibilidad con 802.11b. De este modo:

- CWmin = 31
- Tslot = 20 μseg
- SIFS = 10 μseg
- DIFS = 50 μseg

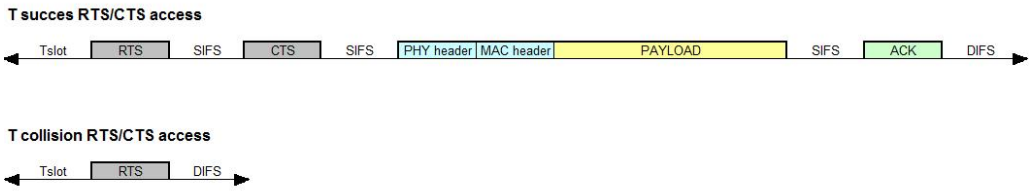

Figura 2.4: DCF usando RTS/CTS

	802.11b		802.11g
CWmin	31		15
CWmax	1023		1023
Tslot	20 microseg		9 microseg
PLCPpreámbulo	144 bits		16 microseg => 96 bits
PLCPheader	48 bits		4 microseg => 24 bits
MACheader	224 bits		224 bits
Header	34 Byte		31 Byte
Tplcp	Tpreamb+cabecera largos	Tpreamb+cabecera cortos	20 microseg
	192 microseg	96 microseg	
C	1 2 5,5 11 (Mbps)		6 9 12 18 24 36 48 54 (Mbps)
SIFS	10 microseg		10 microseg
Ccontrol	1 ó 2 Mbps		6 Mbps
DIFS	50 microseg		28
ACK	112 bit + PLCPheader + PLCPpreamb		112 bit + PLCPheader + PLCPpreamb
ACKtimeout	SIFS + ACK + Tslot + 2d		SIFS + ACK + Tslot + 2d
d	distancia / C		distancia / C

Figura 2.5: Parámetros de IEEE 802.11b y 802.11g

Otros mecanismos soportados en 802.11

En este apartado se describe brevemente el mecanismo de acceso RTS/CTS y el mecanismo de la fragmentación.

- *RTS/CTS*: Para que una estación mande información antes debe mandar una trama RTS. Cuando al receptor le llega esta trama contesta con un CTS para informar que esta preparado para recibir la siguiente transacción. Esta información se tiene en cuenta para decidir si el medio está ocupado.

- *Fragmentación y reensamblado* Las razones para fragmentar en WLANs son dos:

  1. Probabilidad de error.

  2. Paquetes más pequeños representan menor sobrecarga en caso de ser retransmitidos.

Para no cambiar el interfaz al nivel LLC, se fragmenta a nivel MAC. Su funcionamiento es el de parada y espera.

2.3.2 Canales en 802.11

Cada canal necesita un ancho de banda de 22 Mhz para transmitir la información, por lo que se produce un inevitable solapamiento de varios canales contiguos. Es decir, cada uno de los 14 canales asignados al IEEE 802.11 tiene un ancho de banda de 22 Mhz, y la gama de frecuencias disponible va de los 2.412 GHz hasta los 2.484 GHz. Este espacio es dividido por el IEEE 802.11 en 14 canales, es decir, si bien cada canal es de 22 Mhz, para la totalidad de los 14 canales estamos asignando tan solo 72 MHz en lugar de los 308 MHz necesarios. Para evitar interferencias en presencia de varios puntos de acceso cercanos, estos deberían estar en canales no solapables.

En la siguiente imágen se muestra como canales próximos causan interferencia entre si, pues en la frecuencia del 2.4 GHz solo hay tres canales completos (1, 6 y 11) y los demás se solapan entre si, es decir, dos canales no completos y contiguos comparten algunas frecuencias:

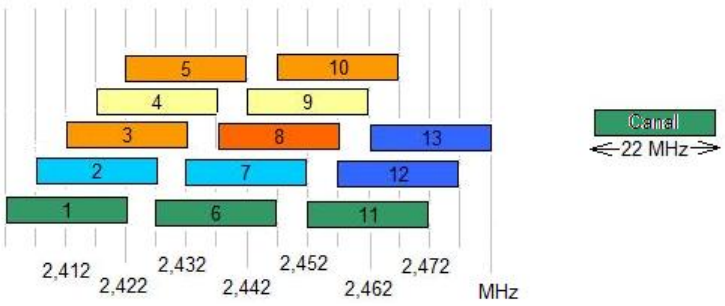

Figura 2.6: Información de canales para redes 802.11b/802.11g

A continuación se resumen la familia de especificaciones que se consideran más interesantes para el concepto de este proyecto. Estas son 802.11a, 802.11b, 802.11g, 802.11k (que servirá para entender alguno de los trabajos futuros) y 802.11s.

2.3.3 802.11a

Extensión del 802.11 que se aplica a redes LAN y provee una velocidad de hasta 54 Mbps en la banda de 5 GHz. Utiliza 52 subportadoras orthogonal frequency-division multiplexing (OFDM). A pesar de la velocidad que ofrece los equipos que trabajan con este estándar no pueden penetrar tan lejos como los del estándar 802.11b dado que sus ondas son más fácilmente absorbidas. Además no es compatible con 802.11b y 802.11g. Esta tecnología de velocidad mayor que 802.11b permite que las redes locales inalámbricas tengan un mejor rendimiento para aplicaciones multimedia.

2.3.4 802.11b

El protocolo 802.11b fue el más utilizado hace unos años hasta que 802.11gse hizo con el mercado actual. Ofrece un rendimiento total máximo de 11 Mpbs (6 Mpbs en la práctica) y tiene un alcance de hasta 300 metros en un espacio abierto. Utiliza el rango de frecuencia de 2,4 GHz con tres canales de radio disponibles. 802.11b transmite datos en el intervalo de frecuencias ISM (industrial, científico y médico).

2.3.5 802.11g

El objetivo de 802.11g fue desarrollar una mayor velocidad en la capa física a la de 802.11b. Además este estándar debía ser compatible con el estándar IEEE 802.11b. Es decir, la versión 802.11g ha conseguido que el actual índice de transmisión de datos de 11 Mpbs empleado por la versión ‘802.11b´, pase a ser de 54 Mpbs, lo que permite dar servicio a 4 ó 5 veces más de usuarios y extender el uso de las redes wireless 802.11, conocidas popularmente como WIFI, a servicios bastante demandados como la transmisión inalámbrica de video-multimedia y la difusión de MPEG.

Las unidades 802.11g podrán trabajar también a velocidades de 11 Mpbs, de modo que los dispositivos 802.11b y 802.11g puedan coexistir bajo la misma red. Los dos estándares aplicarán la banda de frecuencia de 2.4 GHZ.

2.3.6 802.11k

El estándar IEEE 802.11 para redes locales inalámbricas (WLAN) asegura la interoperatividad entre conmutadores y puntos de acceso de distintos fabricantes pero no permite a los sistemas WLAN valorar los recursos de radio frecuencia de un cliente, lo que limita la capacidad de un administrador para gestionar eficientemente sus redes. Y esto es justo lo que trata de resolver 802.11k, propuesta de estándar que definirá una serie de informes y peticiones de métricas que detallan las estadísticas del cliente en los Niveles 1 y 2. Como 802.11k está diseñado para ser implementado en software, para soportarlo el equipamiento WLAN sólo requiere ser actualizado. Y, como es lógico, para que el estándar sea efectivo, han de ser compatibles tanto los clientes (adaptadores y tarjetas WLAN) como la infraestructura (puntos de acceso y conmutadores WLAN).

2.3.7 802.11s

Parece que el estandar 802.11s puede acabar con el caos que existe actualmente en el mundo wireless a la hora de montar repetidores. Con la nueva propuesta tecnológica pasaríamos a tener redes malladas (mesh). Tiene el objetivo de establecer con rapidez un estándar para WLANs en malla que permita una comunicación fluida entre los usuarios de dispositivos inalámbricos. Pero este estándar presenta ciertas limitaciones como que sólo usa un canal. Este es un estándar que está en desarrollo.

Capítulo 3

Despliegue del entorno

Se pretende hcer un despliegue con dispositivos comerciales para hacer pruebas sobre redes mesh. Consistirá en dos PC bajo sistema operativo Linux, equipos Linksys WRT54GL y un dispositivo de red inalámbrico instalado en cada PC.

Uno de los PC llevará el nombre de "lapa" y el otro llevará el nombre de "gusano". Estos dos PCs servirán como receptor y emisor de las comunicaciones llevadas a cabo. Comunicaciones que serán como origen uno de los PCs, pasará a un router por la interface cableada, de este router a diversos routers (dependiendo de los saltos que se quieran analizar en la prueba respectiva) por la interface inalámbrica y del último router se pasará por la interface cableada al PC receptor.

En el aula 41F04 del área de Telemática de la universidad Carlos III de Madrid se ha desplegado una red con dispositivos "Linksys WRT54GL" (cuyas características serán analizadas en el capítulo siguiente).

Se dispone de veinticuatro routers Linksys WRT54GL, de los cuales se usarán 12 routers para las pruebas. El rango de direcciones IP de los Linksys va desde la 192.168.200.1 a la dirección IP 192.168.200.24. Como puede verse forman parte de la misma subred y pueden comunicarse unos con otros.

Los routers se han depositado debajo del falso suelo de dicha aula de forma que están repartidos por todo el aula. En la figura mostrada más abajo puede verse dicha disposición.

Todos los routers "Linksys WRT54GL" van conectados a un switch. En un principio se intentaron estructuras jerarquizadas de switches, pero debido a las pobres prestaciones de los equipos intermedios se utilizó un esquema completamente centralizado.

A continuación vemos un esquema del aula y de la distribución de los dispositivos instalados:

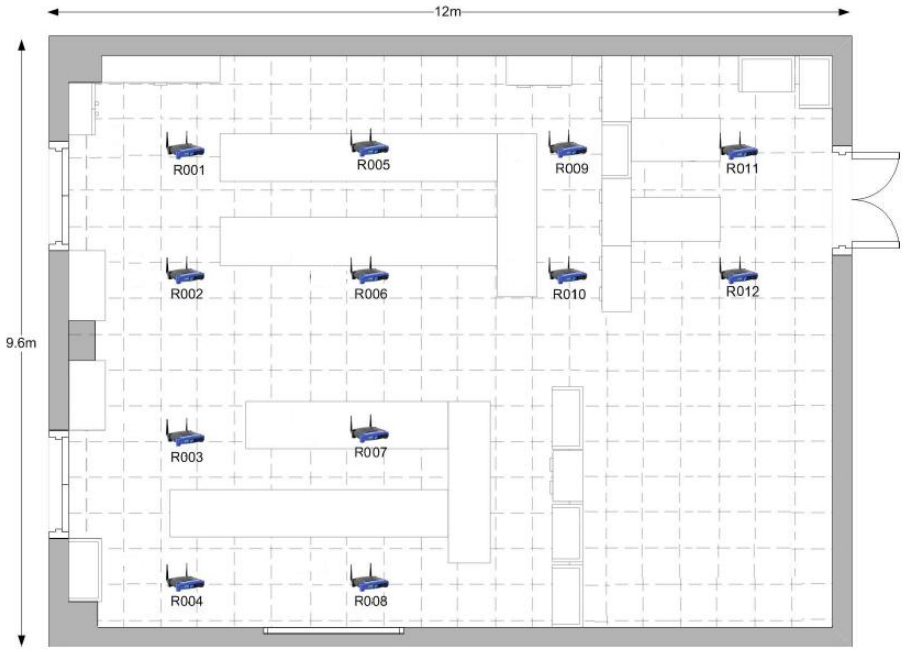

Figura 3.1: Disposición de equipos

Figura 3.2: Equipos en el falso suelo

Para ver una tabla en la cual se muestra la baldosa donde se encuentra

cada dispositivo, así como sus direcciones IP (eth0.1 y wl0) y el nombre de cada dispositivo ir al apéndice.

3.1 Equipos de control y gestión

Cada PC dispone de las siguientes tarjetas:

- Lapa
  - Tarjeta ethernet configurada con la dirección IP 163.117.140.112, máscara de subred 255.255.255.0 y gateway por defecto 163.117.140.2. Se identifica a través de la interfaz eth0.
  - Tarjeta ethernet configurada con la dirección IP 192.168.200.215, con máscara de subred 255.255.255.0. Se identifica a través de la interfaz eth1.
  - Tarjeta ethernet wireless que será configurada con la IP correspondiente y que se identifica a través de la interfaz ath0.
- Gusano
  - Tarjeta ethernet configurada con la dirección IP 163.117.140.112, máscara de subred 255.255.255.0 y gateway por defecto 163.117.140.2. Se identifica a través de la interfaz eth0.
  - Tarjeta ethernet configurada con la dirección IP 192.168.200.210, con máscara de subred 255.255.255.0. Se identifica a través de la interfaz eth1.
  - Tarjeta ethernet wireless que será configurada con la IP correspondiente y que se identifica a través de la interfaz ath0.

En un principio se pensó en un despliegue en el cual cada cuatro routers estuviesen conectados a un switch y, a su vez, esos switches estuviesen conectados a un switch central. Tras varias pruebas se comprobó que los primeros

switches ofrecían bajo rendimiento y se optó por quitarlos usando unicamente el switch principal.

En ambos PCs Se va a instalar el driver "madwifi" para usar la tarjeta inalámbrica Atheros. Se activa el interface a nivel de red, de forma que se podrá gestionar como cualquiera de las interfaces que posee nuestro PC.

Para una explicación más exhaustiva mirar el apéndice de este proyecto.

3.2 Linksys WRT54GL

Linksys, una división de Cisco Systems, Inc., es uno de los más importantes dispositivos en redes Ethernet, inalámbricas y VoIP para el usuario doméstico, SOHO (oficina pequeña, oficina en casa) y para usuarios de pequeñas empresas.

El router WRT54GL de Linksys supone, en realidad, tres dispositivos en uno. En primer lugar, el punto de acceso inalámbrico, que permite conectar dispositivos Wireless-G o Wireless-B a la red. También incorpora un conmutador 10/100 de cuatro puertos completo para conectar dispositivos Ethernet con cables. Puede conectar cuatro PC directamente o encadenar varios concentradores y conmutadores para crear una red que satisfaga sus requisitos. Por último, la función de ruteador une todos los elementos y permite compartir una conexión a Internet DSL o por cable de alta velocidad en toda la red.

Este router esta equipado con un procesador de 200 MHz, posee un interface WLAN de 802.11g y un interface Ethernet de 802.3 conectado a una VLAN dando lugar a un switch de 5 puertos.

Para proteger datos y privacidad, el router puede encriptar todas las transmisiones inalámbricas. Puede funcionar como servidor DHCP, admite paso a través de VPN y se puede configurar para filtrar el acceso a Internet de los usuarios internos.

Gracias a su firmware Linux DD-WRT se le pueden añadir características a este router, aumentando sus posibilidades con respecto al firmware original

de Linksys. Este router viene configurado de fábrica para aceptar cualquier firmware Linux creado por terceros.

Figura 3.3: Linksys

En este caso se eligió el firmware Kamikaze de OpenWrt por ser el firmware más actual. Gracias a este firmware se puede extender la funcionalidad del sistema y, de este modo, acceder a funciones avanzadas consiguiendo un mayor control en la gestión de la red.

Romper el bridge entre LAN y WLAN

Este tipo de routers (Linksys WRT54GL) están configurados por defecto con una interfaz virtual llamada puente (bridge) encargada de conectar dos o más interfaces reales como si perteneciesen a una misma subred. De este modo, en la configuración por defecto, existe un puente entre la interfaz WLAN y los cuatro puertos de redes LAN.

Antes de comenzar a hacer pruebas con el interfaz inalámbrico hay que separar el bridge interno de los routers, ya que éste une el interfaz cable con el inalámbrico; de modo que el tráfico que mandemos se mandará a través del cable y no a través del interfaz inalámbrico que es lo que se busca.

La configuración por defecto es:

Para deshacer el bridge se debe modificar el archivo **/etc/config/network** para dejar las interfaces como se muestra en el cuadro 3.1. Las bocas 2, 3,

Configuración por defecto		
Interface Name	**Description**	**Default Configuration**
br-lan	LAN and WIFI	192.168.1.1/24
vlan0 (eth0.0)	LAN ports (1 to 4)	None
vlan1 (eth0.1)	WAN port	DHCP
wl0	WiFi	Disabled

Cuadro 3.1: Configuración por defecto de los Linksys

4 seran eth0.0; la boca 1 sera eth0.1 y la boca internet sera eth0.2. Posteriormente se instalan unos paquetes que seran útiles, paquetes como ip, wl, iperf...

Y asignamos un nombre a cada router.El nombre asignado a cada router será CMPXXX donde las X representan los tres últimos dígitos de la dirección IP asignada a la interfaz lan del router.

Para una explicación más exhaustiva mirar el apéndice de este proyecto.

3.3 Herramientas utilizadas

En este capítulo se analizarán las herramientas usadas para llevar a cabo las pruebas que se han realizado para la evaluación de la red creada a partir de los dispositivos comerciales "Linksys WRT54GL". Cada herramienta tiene su funcionamiento y se realizará una breve descripción de cada una de ellas.

El proyecto ha sido relizado bajo el sistema operativo Linux, con lo cual las herramientas seleccionadas han sido GNU GPL[1] (herramientas gratuitas).

3.3.1 Supervisión de la red

En esta sección se verán las herramientas que se han usado para la supervisión y gestión de la red.

[1]GNU GPL es una licencia cuyo propósito es declarar que el software cubierto por esta licencia es software libre y protegerlo de intentos de apropiación que restrinjan esas libertades a los usuarios.

Nagios

Nagios es una aplicación open source que nos permite monitorear el estado de los switchs y de los routers en una red que hayamos especificado anteriormente.

Nos alerta cuando algo no va bien y nuevamente cuando está bien. Podemos ver en detalle el estado de nuestra red a través de la interfaz web de Nagios.

Se añaden dispositivos a la red para que él los monitorice. Ya hay plantillas de equipos, grupo de equipos (hostgroups) y servicios, así que lo que se hace es modificar esas plantillas.

A continuación se agregan definiciones de servicio para monitorear pérdidas de paquetes y el promedio de round trip time[2] entre el equipo de Nagios y el router cada 5 minutos.

Para una explicación más exhaustiva mirar el apéndice de este proyecto.

Wireless Tools

Wireless Tools es una colección de programas de la línea de comandos que no solamente sirve información sobre WLANs, sino que también ayuda a configurar conexiones inalámbricas.

Las herramientas que incluye este paquete son las siguientes:

- **iwconfig**: Presenta información sobre configuración y configura interfaces WLAN. Iwconfig es similar al comando ifconfig[3], pero está dedicado a las interfaces inalámbricas. Las opciones más utilizadas del comando iwconfig son el ESSID (o nombre de red), la frecuencia de funcionamiento o canal en el dispositivo, el modo de funcionamiento del dispositivo (Ad-hoc, Master o Monitor) y el rate entre otras opciones.

[2]Round Trip Time se define como el tiempo que tarda un paquete enviado desde un emisor en volver a este mismo emisor habiendo pasado por el receptor de destino

[3]ifconfig es un comando que permite configurar o desplegar numerosos parámetros de las interfaces de red. Si se llama sin argumentos suele mostrar la configuración vigente de las interfaces de red activas.

- **iwlist**: Se utiliza para mostrar información detallada de una interfaz de red inalámbrica, incluida la información que se ha mostrado de iwconfig. Los parámetros más usuales de iwlist son scan que devuelve la lista de puntos de acceso y celdas Ad-Hoc dentro de rango, freq / channel que devuelve la lista de frecuencias disponibles en el dispositivo y el número de canales definidos, rate que lista las tasas de transferencia soportadas por el dispositivo...

- **iwpriv**: Configura varios parámetros específicos de driver. Con iwpriv se le pueden pasar a las tarjetas unos parámetros y configuración específica de cada interfaz (en contraste con iwconfig que presentaba funcionalidades genéricas).

Para una explicación más exhaustiva mirar el apéndice de este proyecto.

Análisis de tráfico

Se han usado dos herramientas para el análisis de tráfico en la red, Wireshark (con interfaz gráfica) y tshark (desde línea de comandos). La función de este tipo de herramientas se basa en "mirar" dentro de los paquetes para mostrar la utilización que se está haciendo del ancho de banda. A continuación se explica más detalladamente cada uno de ellos.

- **Wireshark** Wireshark, antes conocido como Ethereal, es un capturador/-analizador de paquetes de red. Permite ver que paquetes están circulando en la red. Posee una interfaz gráfica y muchas opciones de organización y filtrado de información. Así, permite ver todo el tráfico que pasa a través de una red (usualmente una red Ethernet, aunque es compatible con algunas otras). Las características más destacables de Wireshark son las que se enuncian a continuación:

  - Captura de paquetes en tiempo real desde una intefaz de red.
  - Muestra los paquetes con información detallada.
  - Abre y guarda paquetes capturados.

  - Filtrado de información de paquetes.
  - Resaltado de paquetes dependiendo el filtro.
  - Crear estadísticas.

- **tshark**

  En ocasiones es preferible, o simplemente no se puede, usar la interfaz gráfica que proporciona Wireshark. En estas ocasiones es aconsejable usar la herramienta tshark. Es un analizador de red desde línea de comandos al que también se le pueden aplicar filtros. Esta herramienta se incluye dentro de Wireshark. La salida de tshark se puede volcar a un archivo y posteriomente abrir este archivo con Wireshark. Es una herramienta muy útil a la hora de hacer scripts par automatizar el trabajo, ya que los scripts hacen uso de la línea de comandos.

- **tcpdump** Es otro analizador de red que se cargó en los routers para capturar el tráfico de otras fuentes al hacer pruebas con una transmisión. Al igual que los dos analizadores mencionados a tcpdump también se le pueden añadir filtros que facilitan el trabajo con scripts.

Generador de tráfico: Iperf

Iperf es una herramienta para medir el máximo ancho de banda sobre los protocolos TCP y UDP (en este proyecto se usa el protocolo UDP), permitiendo modificar y optimizar diferentes parámetros. Iperf reporta el BW, perdida de paquetes (para UDP) y el retardo causado por jitter. Todo ello enviando datagramas TCP o UDP, según le especifiquemos, y esperando la respuesta ACK[4].

Con IPerf podemos medir el ancho de banda y rendimiento de una conexión entre dos host. Se trata, pues, de una herramienta cliente-servidor. Con lo cual se tendrá que ejecutar Iperf en dos máquinas. Una hará de Servidor y otra de Cliente. En el caso de este proyecto las máquinas que harán tales funciones

[4]Tramas Acknowledgement (ACK): Las tramas ACK tienen como objetivo confirmar la recepción de una trama.

serán los PCs gusano y lapa, pasando por tantos routers intermedios en el encaminamiento del tráfico como saltos queramos añadir a la prueba realizada.

En modo cliente lanzaremos peticiones a una ip y un puerto que especifiquemos mientras que en modo servidor quedará escuchando peticiones en dicho puerto.

Para una explicación más exhaustiva mirar el apéndice de este proyecto.

Acceso remoto a equipos

Para el acceso remoto a equipos se usó ssh. De este modo se pueden manejar y gestionar los dispositivos mediante un intérprete de comandos. Para poder lanzar scripts que entren remotamente a dichos dispositivos se tuvo que activar ssh sin password. Para conectarse a un servidor vía SSH sin contraseña lo que se hace es crear una clave que permita acceder con la comprobación de las mismas de forma automática. Lo primero, en la máquina cliente se genera una clave RSA, esto preguntará el archivo a guardar y opcionalmente una frase de desafío que se enviará y nos pedirá cada vez que nos conectemos al servidor destino. Esta puede ser en blanco. Una vez hecho esto, se genera el archivo /.ssh/idrsa.pub el cual se debe copiar al servidor que nos queremos conectar sin contraseña.

Como ya se ha dicho, de este modo se puede conectar con los dispositivos sin la necesidad de introducir un password. Es muy útil para elaborar scripts de forma que puedan ser ejecutados remotamente.

Capítulo 4

Análisis de prestaciones

4.1 Aislamiento del falso suelo

Como ya se ha dicho para la elaboración del despliegue se usa el falso suelo que, a parte de proteger fisicamente los dispositivos y con lo cual la red, tambien se supone que tendrá un índice de aislamiento. Para ver el impacto de este aislamiento se hace una prueba en la cual se mide el ancho de banda obtenido con una transmisión UDP durante 30 segundos (esta operación se repite cinco veces) enviando en dos potencias de transmisión distintas. Se realizan dos pruebas, una primera prueba en la cual para la transmisión se coloca un router encima del falso suelo y el segundo router debajo del falso suelo y una segunda prueba en la cual ambos routers se depositan debajo del falso suelo. Se pueden ver los resultados obtenidos en la tabla, donde se comparan estas situaciones. Cuando ambos routers están debajo del falso suelo se obtienen mejores resultados debido a dos causas, el falso suelo atenúa las interferencias causadas por otras transmisiones que están teniendo lugar encima del falso suelo y que cuando la transmisión se realiza con un router encima y otro debajo del falso suelo la señal de esa transmisión en absorvida en parte por el aislamiento del falso suelo.

Potencia de tx	RSSI		Throughput	
	Encima del falso suelo	Debajo del falso suelo	Encima del falso suelo	Debajo del falso suelo
10 dBm	-61,6	-51	10,67	14,1
19 dBm	-57,6	-45,4	11,9	14,3

Figura 4.1: Atenuación debido al aislamiento del falso suelo

4.2 Impacto de la entidad generadora de tráfico

En estas pruebas realizadas los dispositivos Linksys no son los encargados de producir el tráfico, sólo se limitarán a enrutarlo al siguiente destino vía radio. Es decir, el tráfico será generado por uno de los PC (en gusano) pasará por el interface cableado a un router Linksys y éste lo pasará por el interface wifi a otro router Linksys que lo enviará a destino (el otro PC, lapa) por el interface cableado; esto será para el caso de un único salto. En el caso de haber varios saltos participarán en el recorrido más dispositivos Linksys y se comunicarán entre ellos vía wifi.

La razón de generar tráfico de PC a PC es hacer las pruebas bajo condiciones realistas. La generación de tráfico puede ser demasiada carga computacional para la capacidad de la CPU de estos dispositivos.

Para demostrar esto se hace una prueba para 802.11g en el canal 13. Se escoge este canal ya que se ha visto que es el canal donde menos tráfico suele haber. La prueba consiste en medir el ancho de banda en función del tamaño del paquete enviado usando para la generación del tráfico los PCs y repitiendo el experimento usando para la generación de tráfico los routers Linksys. Esta prueba queda reflejada en la siguiente figura en la que además se muestra el funcionamiento teórico:

Como puede verse en la figura:

- El funcionamiento depende en gran medida del dispositivo usado para la generación de tráfico.
- Con tamaños de paquete más grandes se obtienen anchos de banda mayores.
- En aproximadamente 1200 octetos el uso de generar tráfico desde el PC lleva a mejores resultados.

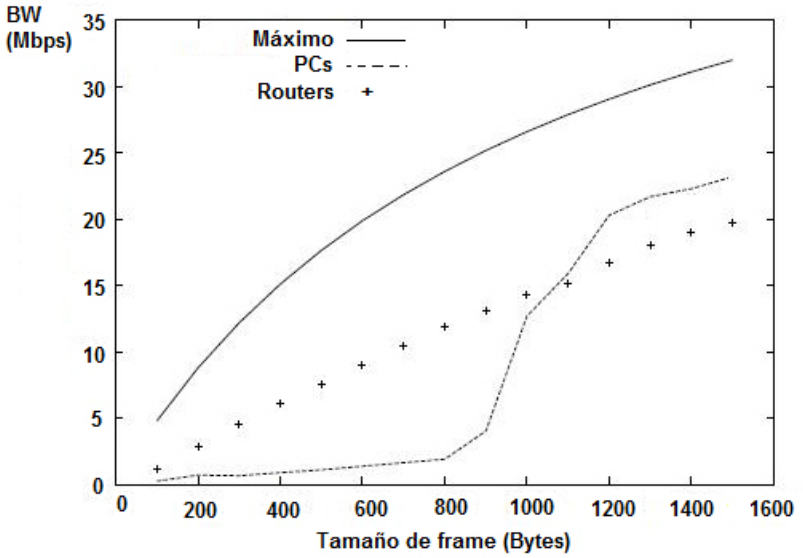

Figura 4.2: Comparación entre generar tráfico con los PCs o con los routers

Como se observa, generar tráfico a partir de los routers funciona mejor cuando el tamaño de los paquetes es menor. Esto se debe a que a menores tamaños de paquetes mayor cantidad de ellos se generan, con lo que generando tráfico con los PCs los routers tienen que recurrir muchas veces a su tabla de routing, este proceso conlleva más tiempo que generar un paquete de poco tamaño ellos mismos y enviarlo por el interfaz adecuado. Esto cambia a partir de unos 1200 Bytes ya que, desde ese punto, es más rentable que los routers recurran a sus tablas de routing que generar ellos mismos los paquetes.

4.3 Relación entre prestaciones y hora del día

Se ha visto que el funcionamiento de 802.11g no está cercano al valor máximo teórico. Se analizan las posibles causas en pruebas sucesivas. Para esta prueba se va a analizar el ancho de banda que ofrece una transmisión de un PC a otro pasando por dos routers conectados entre sí por medio de wifi, es decir de PC a router por el interfaz cableada, de ese router a otro mediante interfaz wifi y de este último al otro PC mediante interfaz cableada. Se analizará el ancho de banda de esa transmisión y los paquetes capturados por otras transmisiones durante dos días, un día entre semana y un día del fin de

semana donde se supone que la cantidad de tráfico que interfiera será menor. Para capturar paquetes de otras transmisiones distintas se recurre a un router. En este router se usa tcpdump para esta labor y un script que filtra la transmisión en curso que se quiere analizar, de modo que sólo se capturen paquetes de otras transmisiones y poder entender el comportamiento de la transmisión en sí.

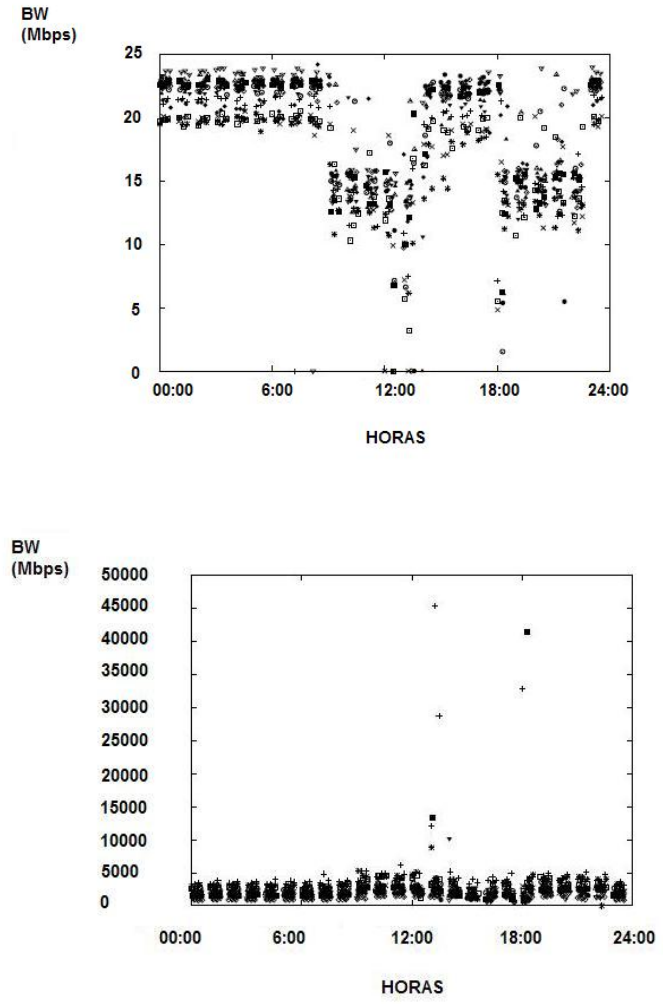

Figura 4.3: Impacto en el ancho de banda un día entre semana

Para la siguiente prueba se realiza una comunicación unidireccional entre dos dispositivos Linksys usando 802.11g. Para ello se genera tráfico con la herramienta iperf desde un PC a otro PC. Se genera tráfico UDP a 30 Mbps durante 30 segundos y se hace la prueba para todos los canales (del canal 1

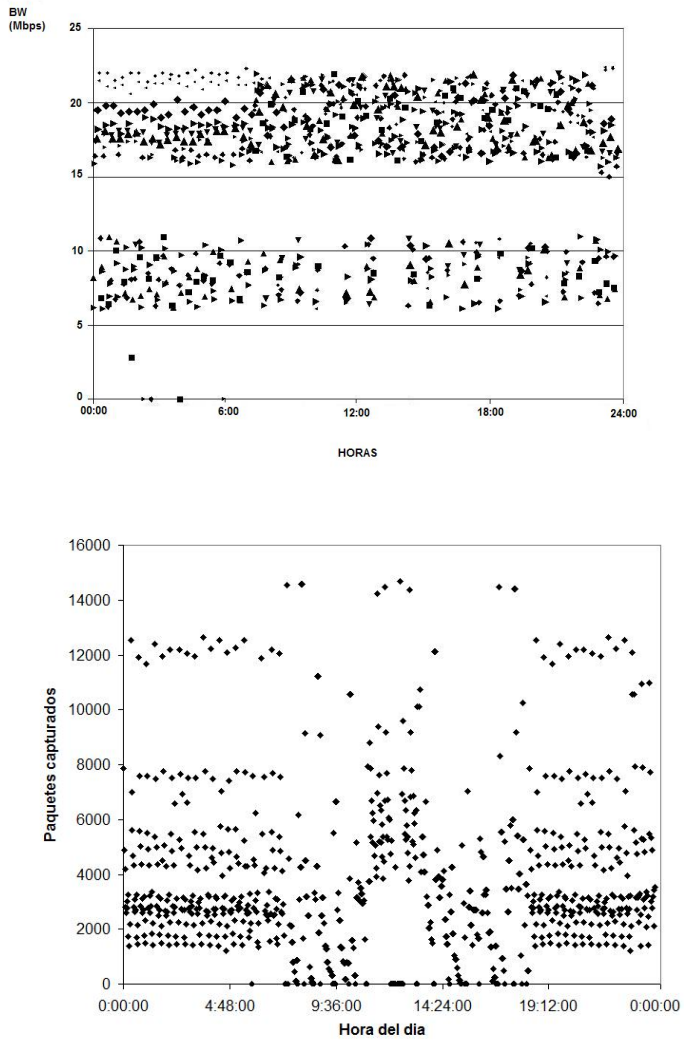

Figura 4.4: Impacto en el ancho de banda un sábado

al 13). Mientras otro router trabaja con tcpdump escuchando las diferentes transmisiones que se producen en el mismo canal.

El comportamiento que sigue esta figura puede ser resumido como sigue:

- Existen dos estados que cambian aproximádamente de 9h a 14h y de 18.5h a 21.5h.
- En el primer estado (de 0h a 9h y de 14h a 18h) el funcionamiento es estable. Se observa el tráfico de otras fuentes y se aprecia que existe menor cantidad de tráfico que interfiera en nuestras medidas que en el segundo estado de la gráfica.

- En el segundo estado el funcionamiento es absolutamente imprevisible e inestable. Esto se debe a que en esas horas hay más estudiantes en el laboratorio haciendo sus propias pruebas.

Se realiza la misma prueba (comunicación unidireccional entre dos dispositivos Linksys usando 802.11g y generando tráfico UDP a 30 Mbps durante 30 segundos con la herramienta iperf desde un PC a otro PC). Esta vez el día elegido es un sábado, donde en la universidad no quedan estudiantes para realizar sus pruebas, a no ser que se hagan en remoto como es este caso.

Como puede verse en este caso sólo tenemos un estado en el que la mayoría de las medidas están en torno a 15-25 Mbps y algunas medidas están por debajo. En la figura del tráfico capturado la gran parte de las medidas están en torno a 3000 paquetes capturados aunque existe una franja horaria (de 10 a 14.30) en la que el tráfico de otras fuentes es mayor. Existen valores en torno a 5-10 Mbps pero es mejor que el comportamiento sea estable a esa tasa que tener una tasa mayor pero inestable. Como se observa en la figura, el fin de semana se presenta más estable debido a la menor afluencia de personas trabajando en el laboratorio.

4.4 Impacto de la potencia de transmisión

Se pretende analizar con esta prueba la conectividad y prestaciones resultantes en función de la potencia transmitida. Para comprobar esto, se hacen pruebas con cada posible salto (es decir para cada posible nodo emisor y para cada posible nodo receptor) en cinco potencias de transmision distintas. Se mide el ancho de banda entre un nodo y los otros once para una comunicación unidireccional UDP de 30 seg con sólo una comunicación activa a la vez. Posteriormente se clasifican los anchos de banda obtenidos de mayor a menor y se representan en la figura.

En la figura se observa que en cualquier potencia de transmisión el ancho de banda es muy similar pudiendo incluso mandar tráfico a una potencia de 1dBm. Con esto puede verse que la potencia de transmisión no es relevante en las transmisiones en 802.11g.

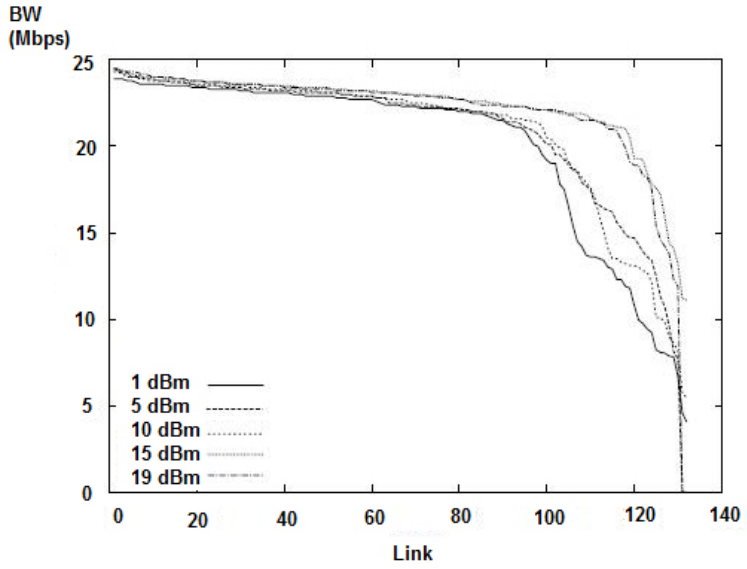

Figura 4.5: Impacto de la Potencia de Transmisión en la conectividad de 802.11g

4.5 Impacto de la distancia

En todas las pruebas se ha tenido en cuenta la influencia que podría ocasionar el campo cercano ya que el campo de radiación que se encuentra cerca de una antena no es igual que el campo de radiación que se encuentra a mayor distancia. En campo cercano se diferencian dos partes: durante la mitad del ciclo, la potencia se irradia desde una antena, en donde parte de la potencia se guarda temporalmente en el campo cercano. Durante la segunda mitad del ciclo, la potencia que esta en el campo cercano regresa a la antena. Esto ocasiona que en campo cercano existan interferencias que no están presentes en campo lejano. Para no tener esas interferencias (con lo cual no estar en campo cercano) se debe cumplir que la distancia física entre dos dispositivos sea mayor o igual a la fórmula:

$d = (2D^2)/\lambda$

Donde D es el diámetro de la antena y landa es la longitud de la onda de radio. Se ha tenido en cuenta la influencia del campo cercano y en todo momento se ha evitado que los dispositivos estuviesen a una distancia menor que d.

Para ver el impacto de la distancia se recurre a dos transmisiones, de modo que una transmisión este en un canal y otra transmisión vaya pasando por diferentes canales. Pero para ver como afecta una transmisión que este en un canal distinto a otra transmisión se deben analizar las transmisiones por separado y después comparar este resultado con el resultado dado por las dos transmisiones en curso simultáneamente. Esta es la prueba que se hará en esta sección y que se explica con más detalle a continuación.

Para analizar el impacto de una fuente de interferencia, se compara el funcionamiento de las dos comunicaciones para dos casos:

- Cuando sólo existe una comunicación (que se define como la configuración 'separado').
- Cuando ambas comunicaciones están en curso simultáneamente (la configuración 'simultaneo').

Entonces, se determina el impacto de la interferencia con la medida siguiente de la eficacia:

BWeff =[Ri(simultaneo) + Rj(simultaneo)]/[Ri(separado) + Rj(separado)]

Donde Ri (separado) es el ancho de banda i cuando no está en curso la comunicación j. Ri (simultaneo) es el ancho de banda de la comunicación i cuando ambas comunicaciones están en curso.

Primero se configuran los canales de las comunicaciones i y j, se fija la misma potencia de transmisión para ambas comunicaciones, se mide el ancho de banda de la comunicación i, después se mide el ancho de banda de la comunicación j y, finalmente, se mide el ancho de banda cuando ambas comunicaciones están en curso simultáneamente. Se repiten las medidas 5 veces.

Una de las comunicaciones se configura en un canal fijo (en este caso en el canal 1) mientras que la otra comunicación se configura en una distancia d (medida en canales). Los resultados obtenidos se plasman en la figura.

En 802.11g existen tres canales ortogonales (a una distancia d=5).

En la figura se observa el siguiente comportamiento:

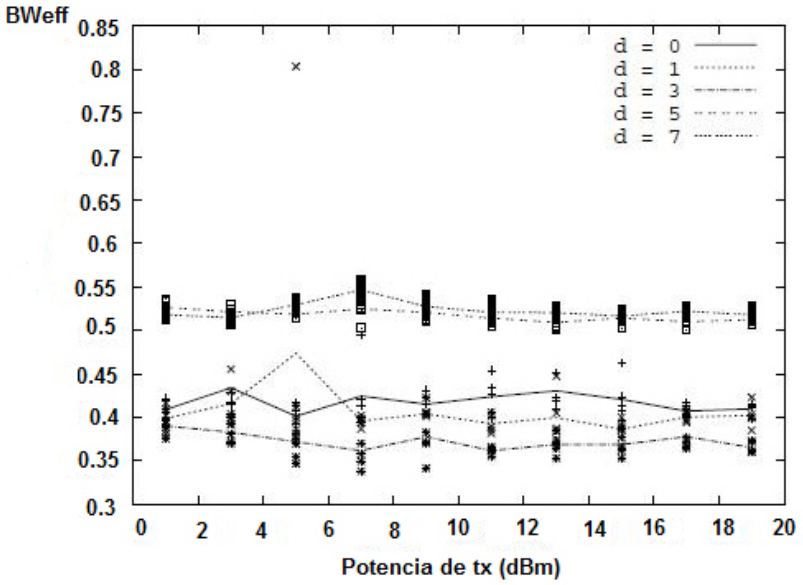

Figura 4.6: Impacto del canal en el ancho de banda

- Para una configuración dada de canales, el funcionamiento no cambia con la potencia de transmisión, las transmisiones pueden llevarse a cabo incluso cuando transmiten en 1 dBm.
- Para d>0 no se garantiza un mejor funcionamiento.
- Incluso el uso de canales ortogonales d = 5 no garantiza independencia en el medio, aunque proporcionen mejores resultados que el caso anterior.

Las conclusiones de esta prueba es que los canales muestran un fuerte solapamiento incluso cuando la distancia entre ellos es mayor a cinco (los canales ortogonales están a una distancia igual a cinco). Con distancias iguales o superiores a cinco existe solapamiento aunque se obtienen resultados mejores.

Capítulo 5

Conclusiones y trabajos futuros

En este capítulo se presentan las conclusiones sacadas de acuerdo a la base teórica expuesta en el proyecto como al comportamiento real de los equipos visto trás la recolección de datos, procesado de los mismos y tras obtener la información que de ellos se generó en las diferentes pruebas realizadas. Obteniendo unos resultados que permiten presentar en la siguiente sección el conjunto de conclusiones.

Posteriormente se enuncia las orientaciones que pueden servir para continuar en un futuro esta línea de investigación y desarrollo.

5.1 Conclusiones

En este proyecto se pretendía obtener información acerca de la calidad en una red mesh, ya que las redes mesh, como ya se ha dicho a lo largo del proyecto es una de las tecnologías emergentes más interesantes en redes inalámbricas.

Los resultados obtenidos muestran las conclusiones citadas a continuación:

- El dispositivo usado para generar y recibir tráfico va a afectar en gran medida al rendimiento de la transmisión. Al generar tráfico de PC a PC se observa que el comportamiento es más irregular y está más alejada de la curva teórica que la curva dibujada cuando son los routers los que

generan el tráfico. Esto cambia cuando se transmiten más de unos 1200 Bytes, ofreciendo mejor resultado cuando la transmisión es de PC a PC. La explicación a este comportamiento es que los routers funcionan mejor generando ellos el tráfico si los paquetes son pequeños ya que se generan muchos paquetes y son más eficientes si no tienen que estar recuriendo a su tabla de encaminamiento. Esto cambia con paquetes grandes ya que los routers, llegados a ese punto, les cuesta más generar tráfico que mirar su tabla de routing y encaminar los paquetes.

- En pruebas sucesivas se ha observado la influencia de otras transmisiones wifi en el rendimiento de la transmisión en cuestión. La cantidad de tráfico que exista en un momento dado va a afectar negativamente a la transmisión haciendo que ésta sea irregular. Se ve afectada aún estando en otros canales debido al solapamiento de los mismos, incluso en canales supuestamente ortogonales como son el canal 1, 6 y 11 el rendimiento mejora pero sigue existiendo solapamiento entre canales.

- Se ha visto que la potencia de transmisión no es un factor importante en el rendimiento en 802.11g. En esa prueba se transmitió en cinco potencias distintas dando resultados muy similares en todas las potencias.

- Todo lo dicho queda reforzado cuando se vió el impacto de la distancia, la potencia de transmisión no es relativamente importante en la transmisión y que el uso de diferentes canales para dos transmisiones simultáneas no garatiza un mejor funcionamiento a no ser que los canales esten a una distancia mayor o igual a cinco, que si llevan a mejores resultados pero no garantizan su independencia (sigue existiendo solapamiento).

5.2 Trabajos futuros

En este proyecto se han realizado una serie de pruebas para medir la calidad de las Mesh. Estas pruebas podrían ayudar al cálculo de parámetros relevantes a la hora de la creación de una red de este tipo.

Este tipo de redes (mesh) cuentan con una serie de características que las hacen muy adecuadas como red de comunicaciones desde el punto de vista de la conectividad.

El principal trabajo futuro sería el uso del tesbed aquí realizado para hacer medidas de los parámetros EDCA (Enhanced Distributed Channel Access).

También podrían hacerse pruebas de routing o realizar estas mismas pruebas en un escenario más real donde la distancia entre routers fuese mayor.

Otro posible trabajo futuro sería analizar más detalládamente el impacto de variar la potencia de transmisión o el canal seleccionado en las transmisiones.

Capítulo 6

Apéndices

En este capítulo se muestran los pasos seguidos para la elaboración del proyecto de un modo más detallado.

6.1 Disposición de los dispositivos

En la tabla se muestra los routers instalados en cada baldosa del falso suelo:

Dirección IP interface eth0.1	Dirección IP inteface wl0	Nombre
192.168.200.1	10.0.200.1	CMP001
192.168.200.2	10.0.200.2	CMP002
192.168.200.3	10.0.200.3	CMP003
192.168.200.4	10.0.200.4	CMP004
192.168.200.5	10.0.200.5	CMP005
192.168.200.6	10.0.200.6	CMP006
192.168.200.7	10.0.200.7	CMP007
192.168.200.8	10.0.200.8	CMP008
192.168.200.9	10.0.200.9	CMP009
192.168.200.10	10.0.200.10	CMP010
192.168.200.11	10.0.200.11	CMP011
192.168.200.12	10.0.200.12	CMP012
192.168.200.13	10.0.200.13	CMP013
192.168.200.14	10.0.200.14	CMP014
192.168.200.15	10.0.200.15	CMP015
192.168.200.16	10.0.200.16	CMP016
192.168.200.17	10.0.200.17	CMP017
192.168.200.18	10.0.200.18	CMP018
192.168.200.19	10.0.200.19	CMP019
192.168.200.20	10.0.200.20	CMP020
192.168.200.21	10.0.200.21	CMP021
192.168.200.22	10.0.200.22	CMP022
192.168.200.23	10.0.200.23	CMP023
192.168.200.24	10.0.200.24	CMP024

Figura 6.1: Tabla disposición de equipos

6.2 Flashear Linksys WRT54GL con Kamikaze

Para cargar el firmware a los routers "Linksys WRT54GL" hemos seguido los siguientes pasos:

1. Reiniciar el router con el cable ethernet en la boca de internet.
2. Cuando se encienda la luz de DMZ apretar el boton reset hasta que esta luz parpadee. El DMZ o zona desmilitarizada se activa cuando no queremos bloquear ni re-direccionar puertos.
3. Abrir un teminal y entrar en el router via: telnet 192.168.1.1. Esta es la dirección IP que por defecto se tiene cuando arrancamos el router de esta forma.
4. En otra terminal hacemos:
   - > cd /tmp/ —> Con este comando nos situamos en la carpeta /tmp/
   - > wget http://downloads.openwrt.org/kamikaze/7.09/brcm-2.4/openwrt-brcm-2.4-squashfs.trx —> de este modo se descarga el firmware.
   - La página oficial del firmware es www.openwrt.org en la que aparte de las imágenes del firmware para descargar, se puede encontrar documentación y un foro en el que resolver los problemas y/o dudas más comunes o que puedan surgir al instalar el firmware.
5. En la terminal que hicimos telnet al router pasamos el firm escribiendo:
   - scp <usuario>@<dirección de eth0>:/tmp/openwrt-brcm-2.4-squashfs.trx /tmp/
   - En nuestro caso concreto la sentencia sería:

     scp mesh@192.168.1.210:/tmp/openwrt-brcm- 2.4-squashfs.trx /tmp/
6. Aplicamos el siguiente comando:

   > mtd write /tmp/openwrt-brcm-2.4-squashfs.trx linux

7. Hacemos un reinicio del router con el comando:

   >reboot

8. Cambiamos el cable ethernet de la boca de internet a la boca 1 y esperamos a que el dispositivo se estabilice. Posteriormente podemos entrar en el router haciendo:

   >telnet 192.168.1.1

   y proceder a cambiar la configuración del mismo.

6.3 Romper el bridge entre LAN y WLAN

En la configuración por defecto, existe un puente entre la interfaz WLAN y los cuatro puertos de redes LAN.

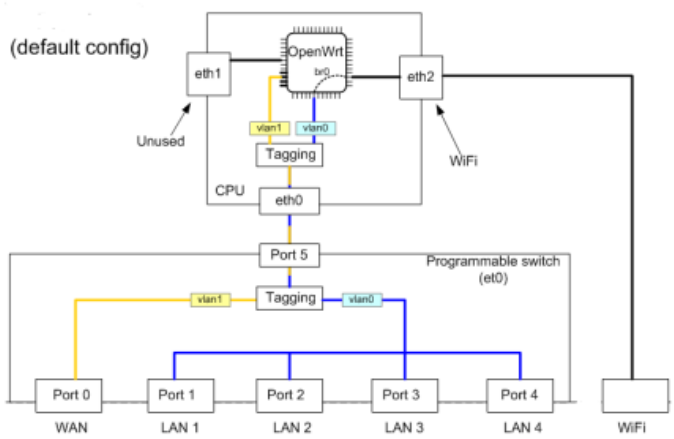

Figura 6.2: Bridge entre LAN y WLAN

La configuración por defecto es:

Para deshacer el bridge en primer lugar se modifica el archivo **/etc/config/network**[1].

[1]Para modificar se ha usado el comando vim, dentro de este comando se ha usado:

- I para pasar a modo texto (en este modo podemos modificar el fichero) y ESC para pasar a modo comando.
- J para suprimir retorno de carro (en modo comando).
- :wq+Enter para guardar los cambios (en modo comando).

Configuración por defecto		
Interface Name	**Description**	**Default Configuration**
br-lan	LAN and WIFI	192.168.1.1/24
vlan0 (eth0.0)	LAN ports (1 to 4)	None
vlan1 (eth0.1)	WAN port	DHCP
wl0	WiFi	Disabled

Cuadro 6.1: Configuración por defecto de los Linksys

Se busca la sección de *config interface lan* y se elimina la línea *option type bridge*. Se cambiará el nombre de br-lan a eth0.0. Posteriormente se añade una nueva sección para configurar la interfaz WiFi:

```
 Wi-Fi LAN configuration
config interface wifi
option ifname "wl0"
option proto static
option ipaddr 192.168.2.1
option netmask 255.255.255.0
```

Y el fichero **/etc/config/wireless** debe tener un aspecto similar a:

```
config wifi-iface
option device wl0
option network wifi
```

Para activar la interfaz wifi sólo bastaría borrar la línea

`option disabled 1.`

El fichero etc/config/networks debe quedar:

```
 VLAN configuration
config switch eth0
option vlan0 "0 1 2 5*"
option vlan1 "3 5"
```

```
option vlan2 ”4 5”
 Loopback configuration
config interface loopback
option ifname ”lo”
option proto static
option ipaddr 127.0.0.1
option netmask 255.0.0.0
 LAN configuration
config interface lan
option ifname ”eth0.0”
option proto static
option ipaddr 192.168.2.1
option netmask 255.255.255.0
 CONF configuration
config interface conf
option ifname ”eth0.1”
option proto static
option ipaddr 192.168.1.1
option netmask 255.255.255.0
 WAN configuration
config interface wan
option ifname ”eth0.2”
option proto dhcp
 Wi-Fi LAN configuration
config interface wifi
option ifname ”wl0”
option proto static
```

```
option ipaddr 192.168.3.1
option netmask 255.255.255.0
```

Las bocas 2, 3, 4 seran eth0.0; la boca 1 sera eth0.1 y la boca internet sera eth0.2.

Y el fichero etc/config/wireless:

```
config wifi-device wl0
option type broadcom
option channel 5
 REMOVE THIS LINE TO ENABLE WIFI: option disabled
1

config wifi-iface
option device wl0
option mode adhoc
option ssid CMesh
option encryption none
```

Se instalan unos paquetes que seran utiles y se desactivan otros que podrían estorbar:

- ipkg update
- ipkg install ip
- ipkg install wl
- ipkg install iperf
- ipkg install ntpclient
- /etc/init.d/dnsmasq stop
- ipkg remove dnsmasq
- /etc/init.d/firewall stop
- rm /etc/init.d/firewall

- /etc/init.d/httpd stop
- rm /etc/init.d/httpd

Y se asigna un nombre a cada router:

> vi etc/config/system

El nombre asignado a cada router será CMPXXX donde las X representan los tres últimos dígitos de la dirección IP asignada a la interfaz lan del router.

6.4 Configuración Nagios

Una vez que hemos descargado este software debemos configurarlo. Lo primero que hacemos es editar el archivo principal de Nagios, para lo que recurrimos a:

- >vi /usr/local/nagios/etc/nagios.cfg

y quitamos la almohadilla de la siguiente línea:

- cfgfile=/usr/local/nagios/etc/objects/switch.cfg

Lo que hacemos con esto es decirle a Nagios que vamos a añadir dispositivos a la red para que él los monitorice. Ya hay plantillas de equipos, grupo de equipos (hostgroups) y servicios, así que lo que se hace es modificar esas plantillas. Para crear esas definiciones de objetos editamos el archivo switch.cfg:

- >vi /usr/local/nagios/etc/objects/switch.cfg

y agregamos esas nuevas definiciones de routers/switches que queremos monitorear. Nagios trata a los routers igual que a los switches. El archivo debe quedar, para añadir un dispositivo, como se muestra a continuación:

- define host

- use generic-switch ; Inherit default values from a template
- hostname linksys-srw224p ; The name we're giving to this switch
- alias Linksys SRW224P Switch ; A longer name associated with the switch
- address 192.168.1.253 ; IP address of the switch
- hostgroups allhosts,switches ; Host groups this switch is associated with

Cambiando los campos hostname, alias y address por los valores de cada dispositivo.

A continuación agregamos definiciones de servicio para monitorear pérdidas de paquetes y el promedio de round trip time entre el equipo de Nagios y el router cada 5 minutos. Esto es:

- define service
- use generic-service ; Inherit values from a template
- hostname linksys-srw224p ; The name of the host the service is associated with
- servicedescription PING ; The service description
- checkcommand checkping!200.0,20 % !600.0,60 % ; The command used to monitor the service>
- normalcheckinterval 5 ; Check the service every 5 minutes under normal conditions
- retrycheckinterval 1 ; Re-check the service every minute until its final/hard state is determined

Este servicio será:

- CRITICO (CRITICAL) si el promedio de round trip (RTA) es mayor a 600 milisegundos o la pérdida de paquetes es 60 % o más.

- PRECAUCIÓN (WARNING) si el RTA es mayor a 200 ms o la pérdida de paquetes es 20 % o más.
- OK si el RTA es menor a 200 ms y la pérdida de paquetes es menor a 20 %.

De este modo sabemos el estado de la red de un modo casi instantáneo.

6.5 Herramientas utilizadas

A continuación se describirán más detalladamente las herramientas que hemos usado en este proyecto.

- **iwconfig**

  Iwconfig es similar al comando ifconfig[2], pero está dedicado a las interfaces inalámbricas. Se utiliza para establecer los parámetros de la interfaz de red que son específicas de la operación inalámbrica. A continuación se describen las opciones más utilizadas del comando iwconfig:

  - **ESSID:** Establece el ESSID (o nombre de red). El ESSID se utiliza para identificar las células que forman parte de la misma red inalámbrica.
  - **Freq / canal:** Establece la frecuencia de funcionamiento o canal en el dispositivo. La frecuencia libre que comprende la banda de 2,4 Ghz utilizada por los dispositivos wireless está subdividida en canales, que varían de acuerdo a las leyes de los diferentes países que los regulan.
  - **Mode:** Establezca el modo de funcionamiento del dispositivo:

[2]ifconfig es un comando que permite configurar o desplegar numerosos parámetros de las interfaces de red. Si se llama sin argumentos suele mostrar la configuración vigente de las interfaces de red activas.

        - **Ad-hoc:** red compuesta de una sola célula y sin punto de acceso.
        - **Master:** el nodo es el maestro, en la sincronización actúa como un AP.
        - **Monitor:** el nodo actúa como un monitor pasiva y sólo recibe los paquetes.
    - **Rate:** Es la velocidad a la que los bits se transmiten en el medio.

- **iwlist**

  Se utiliza para mostrar información detallada de una interfaz de red inalámbrica, incluida la información que se ha mostrado de iwconfig. Los parámetros más usuales de iwlist se muestran a continuación:

    - **scan:** Devuelve la lista de puntos de acceso y celdas Ad-Hoc dentro de rango, y opcionalmente un información sobre ellos (ESSID, calidad, frecuencia, modo).
    - **freq / channel:** Devuelve la lista de frecuencias disponibles en el dispositivo y el número de canales definidos.
    - **rate:** Lista las tasas de transferencia soportadas por el dispositivo.

- **iwpriv**

  Con iwpriv se le pueden pasar a las tarjetas unos parámetros y configuración específica de cada interfaz (en contraste con iwconfig que presentaba funcionalidades genéricas).

6.6 Iperf

A continuación se listan las opciones más usadas en este proyecto:

- **Ambos modos:**

  - -f, –format [kmKM] Formato en el cual quieres recibir el ancho de banda: Kbits, Mbits, KBytes, MBytes.
  - -i, –interval Segundos entre reportes.
  - -p, –port Puerto por el cual se quiere llevar a cabo la comunicación.
  - -u, –udp Usar el protocolo UDP.

- **Modo cliente específicamente:**
  - -b, –bandwidth [KM] Para UDP, ancho de banda a transmitir en bits/sec (por defecto 1 Mbit/sec, necesariamente implica -u)
  - -c, –client <host> Para poner a la máquina en modo cliente conectado a <host>.
  - -n, –num [KM] Número de bytes a transmitir.
  - -t, –time Tiempo en segundos a transmitir (por defecto son 10 segundos).

- **Modo servidor específicamente:**
  - -s, –server Para poner a la máquina en modo servidor.
  - -u, –udp Usar el protocolo UDP.

6.7 Pasos de instalación de la tarjeta Atheros

Se guarda en disco el driver de la tarjeta y se descomprime, en caso de estar comprimido (lo habitual es que este comprimido en .tar), y se compilan los archivos fuente para crear el ejecutable del software que se quiere utilizar.

Descomprimir el archivo: > tar -zxvf madwifi-0.9.4.tar.gz

Cambiarse a la carpeta con los archivos extraídos: > cd madwifi-0.9.4 (Es recomendable leer cualquier archivo readme o install ya que en algunas ocasiones viene información importante para poder iniciar o completar el proceso de instalación).

Se instala la libreria necesaria: sudo apt-get install libc6-dev

Se compila los archivos fuente: > make

Se instala el software compilado: > sudo make install

6.7.1 Configuración de la tarjeta Atheros

Una vez que se tiene lo anterior se carga el módulo (driver) que controla la tarjeta. Los drivers que controlan la tarjeta inalámbrica se gestionan mediante un módulo del kernel que el administrador de la máquina puede activar o desactivar a voluntad. En este caso el nombre del módulo es ath_pci que contiene a su vez una serie de módulos que permiten diferentes acciones como el escanear las redes disponibles. Se carga el módulo:

>sudo modprobe ath_pci

Para que dicho módulo funcione el ordenador ha debido arrancarse en el kernel 2.6.18 o superior (el resto de los kernel no están configurados para el uso de las tarjetas inalámbricas). Para comprobar en que kernel fue arrancado se usa el comando:

>uname -r , o bien, >uname -a

Para comprobar que el módulo se ha cargado correctamente se ejecuta:

>lsmod , o bien usamos, >lsmod | grep ath (con este comando se efectua un filtro para que sólo muestre los módulos que incluyan en el nombre la cadena "ath").

Se pasa a configurar la tarjeta en el modo deseado, para ello se deshabilita el interfaz ath y se vuelve a habilitar en el modo deseado (sta para que funcione como estación , ap para que actúe como punto de acceso o monitor para que actúe en modo monitor):

>sudo wlanconfig ath0 destroy

>sudo wlanconfig ath0 create wlandev wifi0 wlanmode sta

Se activa el interface a nivel de red, de forma que a partir de este momento se podrá gestionar como cualquiera de las interfaces que posee nuestro PC:

>sudo ifconfig ath0 up

Si se desea cambiar el modo de operación de la tarjeta se deben repetir los pasos anteriores.

Para elegir el modo de funcionamiento de la tarjeta (modo 2 ==> modo b; modo 3 ==> modo g) se hace:

>sudo iwpriv ath0 mode 3

Con esto quedaría configurada la tarjeta inalámbrica y con los comandos:

>man iwlist

>man iwconfig

Se obtienen los manuales de como conseguir la suscripción de la tarjeta a una red inalámbrica y configurar los parámetros especiales de wireless.

Capítulo 7

Referencias

- OpenWrt.org. Kamikaze. http://kamikaze.openwrt.org/docs/openwrt.html
- OpenWrt.org. Descarga de firmware. http://downloads.openwrt.org/
- Meshcube.org. The meshing community website. http://www.meshcube.org/
- IWCONFIG. http://linuxcommand.org/man_pages/iwconfig8.html
- T. S. Rappaport, Wireless Communications Principles and Practices. Prentice Hall PTR.
- Debian IPERF. Package iperf. http://packages.debian.org/unstable/net/iperf
- Sourgeforce. Tcpdump Public Repository. www.tcpdump.org
- Katholieke Universiteit Leuven. Wireless LAN: Simulation. Disponible en: http://homes.esat.kuleuven.be/h239/reports/2001/wlan/simulation.php
- http://www.linksysbycisco.com/
- http://www.olsr.org/
- Universidad Carnegie-Mellon. http://www.cmu.edu/computing/wireless/
- Bebea González, Inés María. Geographic routing using a cell structure in wireless ad-hoc networks.
- Akyildiz, Ian Fuat: "Wireless mesh networks"

- http://grouper.ieee.org/groups/802/11/
- http://es.kioskea.net/contents/wifi/wifiintro.php3
- http://www.virusprot.com/Wifi-802.11n-articulo.htm
- http://www.monografias.com/trabajos6/ante/ante.shtml
- http://www.briveira.com/blog/2007/02/07/interferencias-con-el-wifi/
- http://dns.bdat.net/seguridad_en_redes_inalambricas/c113.html